# Linux环境下搭建ftp服务器

安装环境：CentOS 5、6 操作系统

## 一、安装：

### **1.1、安装vsftpd服务相关部件：**

[root@KcentOS5 ~]# yum install vsftpd\*  
Dependencies Resolved======================================================================  
Package                 Arch       Version          Repository        Size  
=============================================================================  
Installing:  
vsftpd                  i386       2.0.5-10.el5     base              137 kTransaction Summary  
=============================================================================  
Install      1 Package(s)  
Update       0 Package(s)  
Remove       0 Package(s)

Installed:

vsftpd.i686 0:2.2.2-11.el6\_4.1

Complete!

### **1.2、确认安装PAM服务相关部件：**

[root@KcentOS5 ~]# yum install pam\*  
Dependencies Resolved  
=============================================================================  
Package                 Arch       Version          Repository        Size  
=============================================================================  
Installing:  
pam-devel               i386       0.99.6.2-3.14.el5 base              186 kTransaction Summary  
=============================================================================  
Install      1 Package(s)  
Update       0 Package(s)  
Remove       0 Package(s)

Installed:

pam-devel.i686 0:1.1.1-13.el6 pam\_pkcs11.i686 0:0.6.2-12.1.el6 pam\_ssh\_agent\_auth.i686 0:0.9.3-84.1.el6

Dependency Installed:

pcsc-lite-libs.i686 0:1.5.2-13.el6\_4

Updated:

pam.i686 0:1.1.1-13.el6 pam\_krb5.i686 0:2.3.11-9.el6 pam\_ldap.i686 0:185-11.el6

Complete!  
开发包，其实不装也没有关系，主要的目的是确认PAM。

### **1.3、安装DB4部件包：**

这里要特别安装一个db4的包，用来支持文件数据库。  
[root@KcentOS5 ~]# yum install db4\*  
Dependencies Resolved  
=============================================================================  
Package                 Arch       Version          Repository        Size  
=============================================================================  
Installing:  
db4-devel               i386       4.3.29-9.fc6     base              2.0 M  
db4-java                i386       4.3.29-9.fc6     base              1.7 M  
db4-tcl                 i386       4.3.29-9.fc6     base              1.0 M  
db4-utils               i386       4.3.29-9.fc6     base              119 kTransaction Summary  
=============================================================================  
Install      4 Package(s)  
Update       0 Package(s)  
Remove       0 Package(s)

Installed:

db4-devel-static.i686 0:4.7.25-18.el6\_4 db4-java.i686 0:4.7.25-18.el6\_4 db4-tcl.i686 0:4.7.25-18.el6\_4

Updated:

db4.i686 0:4.7.25-18.el6\_4 db4-cxx.i686 0:4.7.25-18.el6\_4 db4-devel.i686 0:4.7.25-18.el6\_4

db4-utils.i686 0:4.7.25-18.el6\_4

Complete!

## 二、vsftpd文件配置

vsftpd使用多用户需要有宿主用户，可以按照2.1的步骤建立用户，也可以直接使用现有用户，2.1的介绍可以略过。

### **2.1、建立用户**

**建立vsftpd服务的宿主用户：**

**[root@KcentOS5 ~]# useradd vsftpd -s /sbin/nologin**

默认的vsftpd的服务宿主用户是root，但是这不符合安全性的需要。这里建立名字为vsftpd的用户，用他来作为支持vsftpd的服务宿主用户。由于该用户仅用来支持vsftpd服务用，因此没有许可他登陆系统的必要，并设定他为不能登陆系统的用户。

建立vsftpd虚拟宿主用户：

**[root@KcentOS5 nowhere]# useradd user-name -s /sbin/nologin**

虚拟用户并不是系统用户，也就是说这些FTP的用户在系统中是不存在的。他们的总体权限其实是集中寄托在一个在系统中的某一个用户身上的，所谓vsftpd的虚拟宿主用户，就是这样一个支持着所有虚拟用户的宿主用户。由于他支撑了FTP的所有虚拟的用户，那么他本身的权限将会影响着这些虚拟的用户，因此，处于安全性的考虑，也要非分注意对该用户的权限的控制，该用户也绝对没有登陆系统的必要，这里也设定他为不能登陆系统的用户。（这里插一句：原本在建立上面两个用户的时候，想连用户主路径也不打算给的。本来想加上 -d /home/nowhere 的，据man useradd手册上讲述：“       -d, --home HOME\_DIR  
The new user will be created using HOME\_DIR as the value for the  
user鈙 login directory. The default is to append the LOGIN name to  
BASE\_DIR and use that as the login directory name. The directory  
HOME\_DIR does not have to exist but will not be created if it is  
missing.  
使用-d参数指定用户的主目录，用户主目录并不是必须存在的。如果没有存在指定的目录的话，那么它将不会被建立”。

### **2.2、修改vsftpd的配置文件：**

#### **2.2.1、编辑主配置文件vsftpd.conf**

修改配置文件前，先进行备份。

**[root@KcentOS5 ~]# cp /etc/vsftpd/vsftpd.conf /etc/vsftpd/vsftpd.conf.backup2**

**[root@KcentOS5 ~]# vim /etc/vsftpd/vsftpd.conf**

这里我将原配置文件的修改完全记录，凡是修改的地方我都会保留注释原来的配置。其中加入我对每条配置项的认识，对于一些比较关键的配置项这里我做了我的观点，并且原本英语的说明我也不删除，供参考对比用。  
------------------------------------------------------------------------------  
# Example config file /etc/vsftpd/vsftpd.conf

#

# The default compiled in settings are fairly paranoid. This sample file

# loosens things up a bit, to make the ftp daemon more usable.

# Please see vsftpd.conf.5 for all compiled in defaults.

#

# READ THIS: This example file is NOT an exhaustive list of vsftpd options.

# Please read the vsftpd.conf.5 manual page to get a full idea of vsftpd's

# capabilities.

# Allow anonymous FTP? (Beware - allowed by default if you comment this out).  
#anonymous\_enable=YES  
anonymous\_enable=NO  
设定不允许匿名访问  
#  
# Uncomment this to allow local users to log in.  
local\_enable=YES  
设定本地用户可以访问。注意：主要是为虚拟宿主用户，如果该项目设定为NO那么所有虚拟用户将无法访问。  
#  
# Uncomment this to enable any form of FTP write command.  
write\_enable=YES  
设定可以进行写操作。  
#  
# Default umask for local users is 077. You may wish to change this to 022,  
# if your users expect that (022 is used by most other ftpd's)  
local\_umask=022  
设定上传后文件的权限掩码。

**userlist\_enable=YES**

**userlist\_deny=YES**

**userlist\_file=/etc/vsftpd/user\_list**

**后添加的参数，不确定可用性。**

#  
# Uncomment this to allow the anonymous FTP user to upload files. This only  
# has an effect if the above global write enable is activated. Also, you will  
# obviously need to create a directory writable by the FTP user.  
#anon\_upload\_enable=YES  
anon\_upload\_enable=NO  
禁止匿名用户上传。  
#  
# Uncomment this if you want the anonymous FTP user to be able to create  
# new directories.  
#anon\_mkdir\_write\_enable=YES  
anon\_mkdir\_write\_enable=NO  
禁止匿名用户建立目录。  
#  
# Activate directory messages - messages given to remote users when they  
# go into a certain directory.  
dirmessage\_enable=YES  
设定开启目录标语功能。  
#  
# Activate logging of uploads/downloads.  
xferlog\_enable=YES  
设定开启日志记录功能。  
#  
# Make sure PORT transfer connections originate from port 20 (ftp-data).  
connect\_from\_port\_20=YES  
设定端口20进行数据连接。  
#  
# If you want, you can arrange for uploaded anonymous files to be owned by  
# a different user. Note! Using "root" for uploaded files is not  
# recommended!  
#chown\_uploads=YES

设定禁止上传文件更改宿主。  
#chown\_username=whoever  
#  
# You may override where the log file goes if you like. The default is shown  
# below.  
xferlog\_file=/var/log/vsftpd.log  
设定vsftpd的服务日志保存路径。注意，该文件默认不存在。必须要手动touch出来，并且由于这里更改了vsftpd的服务宿主用户为手动建立的vsftpd。必须注意给与该用户对日志的写入权限，否则服务将启动失败。  
#  
# If you want, you can have your log file in standard ftpd xferlog format  
xferlog\_std\_format=YES  
设定日志使用标准的记录格式。  
#  
# You may change the default value for timing out an idle session.  
#idle\_session\_timeout=600  
设定空闲连接超时时间，这里使用默认。将具体数值留给每个具体用户具体指定，当然如果不指定的话，还是使用这里的默认值600，单位秒。  
#  
# You may change the default value for timing out a data connection.  
#data\_connection\_timeout=120  
设定单次最大连续传输时间，这里使用默认。将具体数值留给每个具体用户具体指定，当然如果不指定的话，还是使用这里的默认值120，单位秒。  
#  
# It is recommended that you define on your system a unique user which the  
# ftp server can use as a totally isolated and unprivileged user.  
#nopriv\_user=ftpsecure  
**nopriv\_user=user-name**  
设定支撑vsftpd服务的宿主用户为手动建立的vsftpd用户。注意，一旦做出更改宿主用户后，必须注意一起与该服务相关的读写文件的读写赋权问题。比如日志文件就必须给与该用户写入权限等。  
#  
# Enable this and the server will recognise asynchronous ABOR requests. Not  
# recommended for security (the code is non-trivial). Not enabling it,  
# however, may confuse older FTP clients.  
async\_abor\_enable=YES  
设定支持异步传输功能。  
#  
# By default the server will pretend to allow ASCII mode but in fact ignore  
# the request. Turn on the below options to have the server actually do ASCII  
# mangling on files when in ASCII mode.  
# Beware that on some FTP servers, ASCII support allows a denial of service  
# attack (DoS) via the command "SIZE /big/file" in ASCII mode. vsftpd  
# predicted this attack and has always been safe, reporting the size of the  
# raw file.  
# ASCII mangling is a horrible feature of the protocol.  
ascii\_upload\_enable=YES  
ascii\_download\_enable=YES  
设定支持ASCII模式的上传和下载功能。  
#  
# You may fully customise the login banner string:  
ftpd\_banner=This vsftp server supports virtual users ^\_^  
设定vsftpd的登陆标语。  
#  
# You may specify a file of disallowed anonymous e-mail addresses. Apparently  
# useful for combatting certain DoS attacks.  
#deny\_email\_enable=YES  
# (default follows)  
#banned\_email\_file=/etc/vsftpd/banned\_emails  
#  
# You may specify an explicit list of local users to chroot() to their home  
# directory. If chroot\_local\_user is YES, then this list becomes a list of  
# users to NOT chroot().

#chroot\_local\_user=YES  
#chroot\_list\_enable=YES  
chroot\_list\_enable=NO  
禁止用户登出自己的FTP主目录。  
# (default follows)  
#chroot\_list\_file=/etc/vsftpd/chroot\_list  
#  
# You may activate the "-R" option to the builtin ls. This is disabled by  
# default to avoid remote users being able to cause excessive I/O on large  
# sites. However, some broken FTP clients such as "ncftp" and "mirror" assume  
# the presence of the "-R" option, so there is a strong case for enabling it.  
#ls\_recurse\_enable=YES  
ls\_recurse\_enable=NO  
禁止用户登陆FTP后使用"ls -R"的命令。该命令会对服务器性能造成巨大开销。如果该项被允许，那么挡多用户同时使用该命令时将会对该服务器造成威胁。  
# When "listen" directive is enabled, vsftpd runs in standalone mode and  
# listens on IPv4 sockets. This directive cannot be used in conjunction  
# with the listen\_ipv6 directive.  
listen=YES  
设定该Vsftpd服务工作在StandAlone模式下。顺便展开说明一下，所谓StandAlone模式就是该服务拥有自己的守护进程支持，在ps -A命令下我们将可用看到vsftpd的守护进程名。如果不想工作在StandAlone模式下，则可以选择SuperDaemon模式，在该模式下 vsftpd将没有自己的守护进程，而是由超级守护进程Xinetd全权代理，与此同时，Vsftp服务的许多功能将得不到实现。  
#  
# This directive enables listening on IPv6 sockets. To listen on IPv4 and IPv6  
# sockets, you must run two copies of vsftpd whith two configuration files.  
# Make sure, that one of the listen options is commented !!  
#listen\_ipv6=YES

**pam\_service\_name=vsftpd**  
设定PAM服务下vsftpd的验证配置文件名。因此，PAM验证将参考/etc/pam.d/下的vsftpd文件配置。  
userlist\_enable=YES  
设定userlist\_file中的用户将不得使用FTP。  
tcp\_wrappers=YES  
设定支持TCP Wrappers。#KC: The following entries are added for supporting virtual ftp users.

**以下这些是关于Vsftpd虚拟用户支持的重要配置项目。默认Vsftpd.conf中不包含这些设定项目，需要自己手动添加配置。**

guest\_enable=YES  
设定启用虚拟用户功能。  
guest\_username=user-name  
指定虚拟用户的宿主用户。  
virtual\_use\_local\_privs=YES  
设定虚拟用户的权限符合他们的宿主用户。  
user\_config\_dir=/etc/vsftpd/user-config.d  
设定虚拟用户个人vsftp的配置文件存放路径。也就是说，这个被指定的目录里，将存放每个Vsftp虚拟用户个性的配置文件，一个需要注意的地方就是这些配置文件名必须和虚拟用户名相同。  
-------------------------------------------------------------------------  
保存退出。

#### **2.2.2、建立vsftpd的日志文件，并更该属主为vsftpd的服务宿主用户：**

[root@KcentOS5 ~]# touch /var/log/vsftpd.log  
[root@KcentOS5 ~]# chown vsftpd.vsftpd /var/log/vsftpd.log

#### **2.2.3、建立虚拟用户配置文件存放路径：**

[root@KcentOS5 ~]# mkdir /etc/vsftpd/ user-config.d /

### 2.3、虚拟用户配置

#### **2.3.1、编写配置文件**

进入vsftpd.conf文件中user\_config\_dir指定的目录

[root@KcentOS5 ~]# vi /etc/vsftpd/user-config.d /user-name  
--------------------------------  
local\_root=/home/user-name

write\_enable=YES

download\_enable=Yes

local\_umask=022

anonymous\_enable=NO

anon\_upload\_enable=NO

anon\_world\_readable\_only=NO

anon\_mkdir\_write\_enable=YES

anon\_other\_write\_enable=YES

**注意：文件名与3.1中创建的虚拟用户的文件名对应。**

这里将原vsftpd.conf配置文件经过简化后保存作为虚拟用户配置文件的模版。这里将并不需要指定太多的配置内容，主要的框架和限制交由 vsftpd的主配置文件vsftpd.conf来定义，即虚拟用户配置文件当中没有提到的配置项目将参考主配置文件中的设定。而在这里作为虚拟用户的配置文件模版只需要留一些和用户流量控制，访问方式控制的配置项目就可以了。这里的关键项是local\_root这个配置，用来指定这个虚拟用户的FTP主路径。

#### **2.3.2、权限检查**

**查看宿主用户是否有访问相应文件的权限**

[root@KcentOS5 ~]# ll /home/user-name

total 24  
drwxr-xr-x 2 user-name user-name 4096 Sep 16 05:14 kanecruise  
drwxr-xr-x 2 user-name user-name 4096 Sep 16 05:00 mello  
drwxr-xr-x 2 user-name user-name 4096 Sep 16 05:00 near

## 三、制作虚拟用户数据库文件

### 3.1、建立虚拟用户名单文件：

**[root@KcentOS5 ~]# touch /etc/vsftpd/virtusers**

建立了一个虚拟用户名单文件，这个文件就是来记录vsftpd虚拟用户的用户名和口令的数据文件，我这里给它命名为virtusers。为了避免文件的混乱，把这个名单文件就放置在/etc/vsftpd/下。

**[root@KcentOS5 ~]# vi /etc/vsftpd/virtusers**

----------------------------  
kanecruise  
123456  
near  
123456near  
mello  
123456mello  
----------------------------  
编辑这个虚拟用户名单文件，在其中加入用户的用户名和口令信息。格式很简单：“一行用户名，一行口令”。

### 3.2、生成虚拟用户数据文件：

**[root@KcentOS5 ~]# db\_load -T -t hash -f /etc/vsftpd/virtusers /etc/vsftpd/virtusers.db**

这里我顺便把这个命令简单说明一下  
----------------------------------------------------------------------  
察看db4的db\_load命令使用方法：  
[root@KSRV2 vsftpd]# db\_load  
usage: db\_load [-nTV] [-c name=value] [-f file]  
[-h home] [-P password] [-t btree | hash | recno | queue] db\_file  
usage: db\_load -r lsn | fileid [-h home] [-P password] db\_file  
解释在本篇中，db\_load命令几个相关选项很参数-T  
The -T option allows non-Berkeley DB applications to easily load text files into databases.  
If the database to be created is of type Btree or Hash, or the keyword keys is specified as set, the input must be paired lines of text, where the first line of the pair is the key item, and the second line of the pair is its corresponding data item. If the database to be created is of type Queue or Recno and the keywork keys is not set, the input must be lines of text, where each line is a new data item for the database.  
选项-T允许应用程序能够将文本文件转译载入进数据库。由于我们之后是将虚拟用户的信息以文件方式存储在文件里的，为了让Vsftpd这个应用程序能够通过文本来载入用户数据，必须要使用这个选项。If the -T option is specified, the underlying access method type must be specified using the -t option.  
如果指定了选项-T，那么一定要追跟子选项-t-t  
Specify the underlying access method. If no -t option is specified, the database will be loaded into a database of the same type as was dumped; for example, a Hash database will be created if a Hash database was dumped.  
Btree and Hash databases may be converted from one to the other. Queue and Recno databases may be converted from one to the other. If the -k option was specified on the call to db\_dump then Queue and Recno databases may be converted to Btree or Hash, with the key being the integer record number.  
子选项-t，追加在在-T选项后，用来指定转译载入的数据库类型。扩展介绍下，-t可以指定的数据类型有Btree、Hash、Queue和Recon数据库。这里，接下来我们需要指定的是Hash型。  
----------------------------------------------------------------------------

**察看生成的虚拟用户数据文件**

**[root@KcentOS5 ~]# ll /etc/vsftpd/virtusers.db**

-rw-r--r-- 1 root root 12288 Sep 16 03:51 /etc/vsftpd/virtusers.db

需要特别注意的是，以后再要添加虚拟用户的时候，只需要按照“一行用户名，一行口令”的格式将新用户名和口令添加进虚拟用户名单文件。但是光这样做还不够，不会生效的哦！还要再执行一遍“ db\_load -T -t hash -f 虚拟用户名单文件虚拟用户数据库文件.db ”的命令使其生效才可以！

**注：virtusers.db是以添加用户的形式管理数据，如果想彻底删除之前的数据，需要先将原来的virtusers.db文件删除，再使用指令重新生成。**

### 3.3、PAM验证文件设定

**查看原来的文件**

**[root@KcentOS5 ~]# cat /etc/pam.d/vsftpd**  
----------------------------------------------------------------  
#%PAM-1.0  
session    optional     pam\_keyinit.so    force revoke  
auth       required     pam\_listfile.so item=user sense=deny file=/etc/vsftpd/ftpusers onerr=succeed  
auth       required     pam\_shells.so  
auth       include      system-auth  
account    include      system-auth  
session    include      system-auth  
session    required     pam\_loginuid.so  
----------------------------------------------------------------

在编辑前做好备份

**[root@KcentOS5 ~]# cp /etc/pam.d/vsftpd /etc/pam.d/vsftpd.backup**

**[root@KcentOS5 ~]# vi /etc/pam.d/vsftpd**  
----------------------------------------------------------------  
#%PAM-1.0  
auth    sufficient      /lib/security/pam\_userdb.so     db=/etc/vsftpd/virtusers  
account sufficient      /lib/security/pam\_userdb.so     db=/etc/vsftpd/virtusers

以上两条是手动添加的，内容是对虚拟用户的安全和帐户权限进行验证。这里的auth是指对用户的用户名口令进行验证。这里的account是指对用户的帐户有哪些权限哪些限制进行验证。

其后的sufficient表示充分条件，也就是说，一旦在这里通过了验证，那么也就不用经过下面剩下的验证步骤了。相反，如果没有通过的话，也不会被系统立即挡之门外，因为sufficient的失败不决定整个验证的失败，意味着用户还必须将经历剩下来的验证审核。

再后面的/lib/security/pam\_userdb.so表示该条审核将调用pam\_userdb.so这个库函数进行。最后的db=/etc/vsftpd/virtusers则指定了验证库函数将到这个指定的数据库中调用数据进行验证。

注：将/etc/pam.d/vsftpd原来的内容删掉，然后加入后面两行。确保两个库/lib/security/pam\_userdb.so、/lib/security/pam\_userdb.s是存在的。

## 四、启动服务并测试

### 4.1、启动服务

**修改配置文件后，需要重启vsftpd服务。**

[root@KcentOS5 ~]# service vsftpd start  
starting vsftpd for vsftpd:                                [ OK ]

### 4.2、测试服务

**在虚拟用户目录中预先放入文件：**  
**[root@KcentOS5 ~]# touch /home/user-name/kanecruise/kc.test**

从其他机器作为客户端登陆FTP

[root@Yum ~]# ftp  
ftp> open 192.168.1.22  
Connected to 192.168.1.22.  
220 This Vsftp server supports virtual users ^\_^  
530 Please login with USER and PASS.  
530 Please login with USER and PASS.  
KERBEROS\_V4 rejected as an authentication type  
Name (192.168.1.22:root): kanecruise  
331 Please specify the password.  
Password: 123456  
230 Login successful.  
Remote system type is UNIX.  
Using binary mode to transfer files.

3.测试列单操作  
ftp> ls  
227 Entering Passive Mode (192,168,1,22,220,24)  
150 Here comes the directory listing.  
-rw-r--r--    1 501      501             0 Sep 15 21:14 kc.test  
226 Directory send OK.（目录列单成功）

4.测试上传操作：  
ftp> put  
(local-file) KC.repo  
(remote-file) KC.repo  
local: KC.repo remote: KC.repo  
227 Entering Passive Mode (192,168,1,22,230,1)  
150 Ok to send data.  
226 File receive OK. （上传成功）  
699 bytes sent in 0.024 seconds (29 Kbytes/s)  
ftp>

5.测试建立目录操作：  
ftp> mkdir test  
257 "/opt/vsftp/kanecruise/test" created （目录建立成功）

6.测试下载操作：  
ftp> get kc.test  
local: kc.test remote: kc.test  
227 Entering Passive Mode (192,168,1,22,164,178)  
150 Opening BINARY mode data connection for kc.test (0 bytes).  
226 File send OK.（下载成功）

7.测试超时：  
ftp> dir  
421 Timeout.（超时有效）  
ftp> user  
Not connected.注意:  
在/etc/vsftpd/vsftpd.conf中，local\_enable的选项必须打开为Yes，使得虚拟用户的访问成为可能，否则会出现以下现象：  
----------------------------------  
[root@KcentOS5 ~]# ftp  
ftp> open 192.168.1.22  
Connected to 192.168.1.22.  
500 OOPS: vsftpd: both local and anonymous access disabled!  
----------------------------------  
原因：虚拟用户再丰富，其实也是基于它们的宿主用户user-name的，如果user-name这个虚拟用户的宿主被限制住了，那么虚拟用户也将受到限制。  
**补充：**

500 OOPS:错误

有可能是你的vsftpd.con配置文件中有不能被实别的命令，还有一种可能是命令的YES 或 NO 后面有空格。

我遇到的是命令后面有空格。因为我是用GEDIT来编辑的配置文件

550 权限错误,不能创建目录和文件

**解决方法: 关闭selinux**

# vi /etc/selinux/config

将 SELINUX=XXX -->XXX 代表级别

改为

SELINUX=disabled

重启